UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/785,722	02/16/2001	Hans Christopher Sowa	CM04812H	4254

22917 7590 09/02/2004

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 09/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/785,722	SOWA ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 August 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-94* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

1. On August 25, 2004, talked to attorney over the phone regarding restriction requirement on this application. Attorney elects one (Group 1) of the following two groups without traverse.

2. Restriction to one of the following inventions is required under 35 U.S.C. 121:

3. Claims 1 – 94, drawn to Group 1, classified in class 380, subclass 247 (authentication within a single and across multiple zones).

4. Claims 95 – 98, drawn to Group 2, classified in class 380, subclass 249 (mobile station power-down management).

5. This Office Action only addresses the claimed inventions of Group 1.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

2. The effective filing date for the subject matter defined in the pending claims in this application is 02/16/2001.

Claim Objections

3. Claim 83 is objected to because of the following informalities: "in the even of a fault" should be "in the event of a fault". Appropriate correction is required.

4. Any other claims not addressed by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1 – 6, 8, 10 – 12, 14 – 19, 21 – 27, 29, 31, 32, 34 – 39 and 41 are rejected under 35 U.S.C. 102(e) as being anticipated by "Terrestrial Trunked Radio (TETRA) Voice Plus Data (V+D) Part 7: Security" (EN 300 392-7 V2.0.19, 2000-11), hereinafter referred to as TETRA-2000.

6. As per claim 1, TETRA-2000 teaches a method comprising the steps of: generating a random number, an expected response, and a derived cipher key; forwarding the random number and a random seed to a base station; receiving, from the base station, a response to the random number and the random seed; comparing the response and the expected response; when the response matches the expected response, forwarding the derived cipher key to the base station (TETRA-2000: see for example, Figure 1 and Section 4.1.2).

7. As per claim 16, TETRA-2000 teaches a method performed by any of a base station and comprising the steps of: receiving an authentication request from a mobile station; determining whether to forward the request to an authentication agent; when it is determined to forward the request, forwarding the request to the authentication agent; receiving a random number and a random seed from the authentication agent; forwarding the random number and the random seed to the mobile station; receiving a response to the random number

and the random seed from the mobile station and forwarding the response to the authentication agent; when the authentication agent authenticates the mobile station, receiving a derived cipher key from the authentication agent; encrypting messages to the mobile station and decrypting messages from the mobile station with the derived cipher key. (TETRA-2000: see for example, Section 4.1.1 Line 8 – 10 & Figure 1 and Section 4.1.2: The base station carries out the authentication protocols between the mobile station and authentication agent).

8. As per claim 23, TETRA-2000 teaches a method comprising the steps of: receiving, from a base station, a random number generated by a mobile station; using a random seed, generating a derived cipher key and a response to the random number and forwarding the random seed and the response to the base station; when a positive authentication message is received from the base station, forwarding the derived cipher key to the base station (TETRA-2000: see for example, Figure 2 and Section 4.1.3 & Section 4.1.4).

9. As per claim 36, TETRA-2000 teaches a method performed by a base station and comprising the steps of: receiving a random number from a mobile station; forwarding the random number to an authentication agent; receiving a response to the random number and a random seed from the authentication agent; forwarding the response and the random seed to the mobile station; when the mobile station authenticates the infrastructure, forwarding an authenticated message to the authentication agent; receiving a derived cipher key from the authentication agent; encrypting messages to the mobile station and decrypting

messages from the mobile station with a derived cipher key (TETRA-2000: see for example, Figure 2 and Section 4.1.3 & Section 4.1.4).

10. As per claims 2, 24 and 37, TETRA-2000 teaches the claimed invention as described above (see claims 1, 23 and 36 respectively). TETRA-2000 further teaches when the response does not match the expected response, discarding the derived cipher key without forwarding the derived cipher key to the base station (TETRA-2000: see for example, Section 4.1.2 Line 9 – 10).

11. As per claims 3 and 17, TETRA-2000 teaches the claimed invention as described above (see claims 2 and 16 respectively). TETRA-2000 further teaches sending a failed authentication message to the base station (TETRA-2000: see for example, Section 4.1.2 Line 9 – 10 and Figure 1).

12. As per claims 4 and 25, TETRA-2000 teaches the claimed invention as described above (see claims 2 and 23 respectively). TETRA-2000 further teaches the expected response is generated at least indirectly from the random number and the random seed (TETRA-2000: see for example, Section 4.1.2 and Figure 1).

13. As per claims 5 and 26, TETRA-2000 teaches the claimed invention as described above (see claims 2 and 23 respectively). TETRA-2000 further teaches the derived cipher key is generated at least indirectly from the random number and the random seed (TETRA-2000: see for example, Section 4.1.2 and Figure 1).

14. As per claims 6 and 27, TETRA-2000 teaches the claimed invention as described above (see claims 2 and 23 respectively). TETRA-2000 further

teaches the derived cipher key (DCK) is stored at a visited location register (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 & Line 9 – 10 and Figure 1: TETRA-2000 teaches the protocol exchange and DCK is generated at the authentication center. TETRA-2000 discloses ensuring the A-key (authentication-key) of MS is never visible outside the authentication center. This implies the DCK can be distributed outside the authentication center including VLR, HLR and etc).

15. As per claims 8 and 29, TETRA-2000 teaches the claimed invention as described above (see claims 2 and 23 respectively). TETRA-2000 further teaches the derived cipher key is stored at a home location register (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 & Line 9 – 10 and Figure 1: TETRA-2000 teaches the protocol exchange and DCK is generated at the authentication center. TETRA-2000 discloses ensuring the A-key (authentication-key) of MS is never visible outside the authentication center. This implies the DCK can be distributed outside the authentication center including HLR, VLR and etc).

16. As per claims 10, 18, 31 and 38, TETRA-2000 teaches the claimed invention as described above (see claims 1, 16, 23 and 36 respectively). TETRA-2000 further teaches the steps are performed by a zone controller (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 and Figure 1: TETRA-2000 teaches the protocol exchange is between the authentication center and mobile station. Therefore, it is evident that HLR/VLR (or zone controller) and base station should all be involved to carry out this authentication protocols).

17. As per claims 11, 19, 32 and 39, TETRA-2000 teaches the claimed invention as described above (see claims 1, 16, 23 and 36 respectively). TETRA-2000 further teaches the steps are performed by a visited location register (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 and Figure 1: TETRA-2000 teaches the protocol exchange is between the authentication center and mobile station. Therefore, it is evident that HLR/VLR (or zone controller) and base station should all be involved to carry out this authentication protocols).

18. As per claim 12, TETRA-2000 teaches the claimed invention as described above (see claim 1). TETRA-2000 further teaches the response is generated by a mobile station (TETRA-2000: see for example, Figure 1: RES1 (Response 1) is sent from MS to AuC in Figure 1).

19. As per claims 14, 21, 34 and 41, TETRA-2000 teaches the claimed invention as described above (see claims 1, 16, 23 and 36 respectively). TETRA-2000 further teaches any of a base site and a TETRA site controller takes the place of the base station (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 and Figure 1: TETRA-2000 teaches the protocol exchange is between the authentication center and mobile station. Therefore, it is evident that HLR/VLR (or zone controller) and base station controller should all be involved to carry out this authentication protocols).

20. As per claims 15, TETRA-2000 teaches the claimed invention as described above (see claim 1). TETRA-2000 further teaches receiving, from the base station, a second random number generated by a mobile station;

generating a second derived cipher key and a second response to the second random number and forwarding the second response to the base station; combining the derived cipher key and the second derived cipher key, yielding a third derived cipher key; when a positive authentication message is received from the base station, forwarding the third derived cipher key to the base station (TETRA-2000: see for example, Section 4.2.1 and Figure 6).

21. As per claim 22, TETRA-2000 teaches the claimed invention as described above (see claim 16). TETRA-2000 further teaches receiving a second random number from a mobile station; forwarding the second random number to the authentication agent; receiving a second response to the second random number from the authentication agent; forwarding the second response to the mobile station; when the mobile station authenticates the infrastructure, forwarding an authenticated message to the authentication agent; receiving a second derived cipher key from the authentication agent; encrypting messages to the mobile station and decrypting messages from the mobile station with the second derived cipher key (TETRA-2000: see for example, Figure 2, Section 4.1.3 and Section 4.1.4).

22. As per claim 35, TETRA-2000 teaches the claimed invention as described above (see claim 23). TETRA-2000 further teaches the method is of a mutual authentication process (TETRA-2000: see for example, Section 4.1.4).

23. Claims 42, 68 – 69, 71 – 82 and 87 – 94 are rejected under 35 U.S.C. 102(e) as being anticipated by Matsumoto (Patent Number: 6134431), hereinafter referred to as Matsumoto.

24. As per claim 42, Matsumoto teaches a system comprising: a first system device in a first zone of the system, the first system device comprised of memory for storing:

a. first zone session authentication information (Matsumoto: see for example, Column 5 Line 47 – 55),

b. a first key for encrypting at least one of key material and a part of the first zone session authentication information for transport in real-time to another system device in the first zone (Matsumoto: see for example, Column 24 Line 25 – 28, Column 6 Line 9 – 13 and Column 5 Line 47 – 55), and

c. a second key for encrypting at least a segment of the first zone session authentication information for transport to a system device in a zone other than the first zone (Matsumoto: see for example, Column 24 Line 47 – 65: Matsumoto teaches using different keys when mobile station moves from one zone to another zone);

d. a second system device comprised of memory for storing the first zone session authentication information at least partially in an encrypted form (Matsumoto: see for example, Column 12 Line 35 – 38, Column 12 Line 44 – 46, and Figure 1 Element 111 & Figure 9).

25. As per claim 68, Matsumoto teaches a method comprising the steps of:

a. generating session authentication information for each of a plurality of authentication keys for use in a communication system (Matsumoto: see for example, Column 12 Line 35 – 38);

b. encrypting the session authentication information (Matsumoto: see for example, Column 12 Line 44 – 46, and Figure 1 Element 111 & Figure 9);

c. forwarding the encrypted session authentication information to a storage device for access in a non-real-time manner (Matsumoto: see for example, Column 12 Line 44 -- 46, and Figure 1 Element 111 & Figure 9: Key Database as a storage device for access in a non-real-time manner).

26. As per claim 87, Matsumoto teaches a system comprising:

a. a plurality of first-level system devices, arranged and constructed to encrypt, store, and forward at least some session authentication information in a non-real-time manner (Matsumoto: see for example, Column 12 Line 44 – 46, and Figure 1 Element 111 & Figure 9: Key Database as a storage device for access in a non-real-time manner);

b. a plurality of second-level system devices, arranged and constructed to receive at least a part of the session authentication information from at least one of the plurality of first-level system devices in a real-time manner (Matsumoto: see for example, Column21 Line 64, and Figure 1 Element 109b: Cell station is one type of second-level system devices).

27. As per claim 69, Matsumoto teaches the claimed invention as described above (see claim 68). Matsumoto further teaches comprising the step of storing

the plurality of keys as encrypted data (Matsumoto: see for example, Column 24 Line 31 – 32).

28. As per claim 71, Matsumoto teaches the claimed invention as described above (see claim 68). Matsumoto further teaches the session authentication information is encrypted by a software-based encryption device (software-based encryption device is widely used and well-known in the art).

29. As per claim 72, Matsumoto teaches the claimed invention as described above (see claim 68). Matsumoto further teaches the session authentication information is encrypted with an interkey (Matsumoto: see for example, Column 24 Line 47 – 65: Matsumoto teaches using different keys when mobile station moves from one zone to another zone).

30. As per claim 73, Matsumoto teaches the claimed invention as described above (see claim 68). Matsumoto further teaches the storage device is a user configuration server (Matsumoto: see for example, Figure 14 Element 103-a / 103-b & Element 100 and Column 47 Line 47 – 55: The exchange operates as a configuration server to couple to the key management device to store and distribute session authentication information for each mobile station residing in the system).

31. As per claim 74, Matsumoto teaches the claimed invention as described above (see claim 68). Matsumoto further teaches forwarding, by the storage device, at least a part of the encrypted session authentication information to a first system device at a zone in the communication system in a non-real-time manner (Matsumoto: see for example, Column 12 Line 44 – 46, and Figure 1

Element 111 & Figure 9: Key Database as a storage device for access in a non-real-time manner).

32. As per claim 75, Matsumoto teaches the claimed invention as described above (see claim 74). Matsumoto further teaches the part of the encrypted session authentication information includes session authentication information for at least one mobile station registered at the zone (Matsumoto: see for example, Column 5 Line 50 – 52).

33. As per claim 76, Matsumoto teaches the claimed invention as described above (see claim 74). Matsumoto further teaches forwarding, by the first system device, at least some of the at least a part of the encrypted session authentication information to a home location register at the zone in a non-real-time manner (Matsumoto: see for example, Column 12 Line 44 – 46, and Figure 1 Element 111 & Figure 9: Key Database as a storage device for access in a non-real-time manner).

34. As per claim 77, Matsumoto teaches the claimed invention as described above (see claim 76). Matsumoto further teaches decrypting, by the second system device, the at least some of the at least a part of the encrypted session authentication information, yielding decrypted session authentication information (Matsumoto: see for example, Column 12 Line 35 – 38, Column 12 Line 44 – 46, & Column 24 Line 25 – 28, Column 6 Line 9 – 13 and Column 5 Line 47 – 55 and Column 24 Line 56 – 65: Matsumoto first teaches the authentication information must be stored with encryption form. Matsumoto further teaches each zone uses different encryption / decryption keys and thereby it is evident that encrypted

session authentication information must be decrypted with the first zone ciphering key and then further encrypted with the second zone encryption key).

35. As per claim 78 and 81, Matsumoto teaches the claimed invention as described above (see claim 77 and 78 respectively). Matsumoto further teaches encrypting, by the second system device, at least a part of the decrypted session authentication information, yielding re-encrypted session authentication information (Matsumoto: see for example, Column 12 Line 35 – 38, Column 12 Line 44 – 46 & Column 24 Line 25 – 28, Column 6 Line 9 – 13 and Column 5 Line 47 – 55 and Column 24 Line 56 – 65: Matsumoto first teaches the authentication information must be stored with encryption form. Matsumoto further teaches each zone uses different encryption / decryption keys and thereby it is evident that encrypted session authentication information must be decrypted with the first zone ciphering key and then further encrypted with the second zone encryption key).

36. As per claim 79, Matsumoto teaches the claimed invention as described above (see claim 78). Matsumoto further teaches encrypting at least the part of the decrypted session authentication information comprises the step of encrypting the at least the part of the decrypted session authentication information using an intrakey (Matsumoto: see for example, Column 12 Line 35 – 38, Column 12 Line 44 – 46 & Column 24 Line 25 – 28, Column 6 Line 9 – 13 and Column 5 Line 47 – 55: Matsumoto first teaches the authentication information must be stored with encryption form. Matsumoto further teaches each zone uses different encryption / decryption keys and thereby it is evident

that encrypted session authentication information must be decrypted with the first zone ciphering key (or intrakey)).

37. As per claim 80, Matsumoto teaches the claimed invention as described above (see claim 78). Matsumoto further teaches encrypting at least the part of the decrypted session authentication information comprises the step of encrypting the at least the part of the decrypted session authentication information using an interkey (Matsumoto: see for example, Column 12 Line 35 – 38, Column 12 Line 44 – 46 & Column 24 Line 25 – 28, Column 6 Line 9 – 13 and Column 5 Line 47 – 55 and Column 24 Line 56 – 65: Matsumoto first teaches the authentication information must be stored with encryption form. Matsumoto further teaches each zone uses different encryption / decryption keys and thereby it is evident that encrypted session authentication information must be decrypted with the first zone ciphering key and then further encrypted with the second zone encryption key (or interkey)).

38. As per claim 82, Matsumoto teaches the claimed invention as described above (see claim 78). Matsumoto further teaches the session authentication information comprises at least two keys utilized in an encryption authentication process (Matsumoto: see for example, Column 12 Line 35 – 38, Column 12 Line 44 – 46, and Column 12 Line 35 – 38: Matsumoto teaches each zone uses different encryption / decryption keys and thereby it is evident that encrypted session authentication information must be decrypted with the first zone ciphering key (or intrakey)).

39. As per claim 88, Matsumoto teaches the claimed invention as described above (see claim 87). Matsumoto further teaches at least one of the plurality of first-level system devices generates the session authentication information (Matsumoto: see for example, Column 5 Line 48 – 49).

40. As per claim 89, Matsumoto teaches the claimed invention as described above (see claim 87). Matsumoto further teaches the plurality of second-level system devices authenticates one or more mobile stations in a real-time manner based on the session authentication information (Matsumoto: see for example, Column 5 Line 65 – 67).

41. As per claim 90, Matsumoto teaches the claimed invention as described above (see claim 87). Matsumoto further teaches the plurality of first-level system devices comprises a key management facility, a user configuration server, and at least one zone manager (Matsumoto: see for example, Figure 14 Element 100, Element 103-a/b, Element 110-a/b and Column 12 Line 35 – 53: Matsumoto discloses key server and PBX where each PBX controls its own zone when mobile station moves from one zone to another zone).

42. As per claim 91, Matsumoto teaches the claimed invention as described above (see claim 87). Matsumoto further teaches the plurality of second-level system devices comprises at least one zone controller and at least one base station (Matsumoto: see for example, Figure 14 Element 100, Element 103-a/b, Element 110-a/b, Element 109 and Column 12 Line 35 – 53: Matsumoto discloses key server and PBX where each PBX controls its own zone when mobile station moves from one zone to another zone).

43. As per claim 92, Matsumoto teaches the claimed invention as described above (see claim 87). Matsumoto further teaches at least one of the plurality of first-level system devices is arranged and constructed to encrypt the session authentication information using an interkey (Matsumoto: see for example, Column 24 Line 60 – 65).

44. As per claim 93, Matsumoto teaches the claimed invention as described above (see claim 87). Matsumoto further teaches the plurality of second-level system devices is arranged and constructed to encrypt at least a segment of the session authentication information using an interkey when the encrypted session authentication information is forwarded to a system device in a zone other than the zone in which the forwarding device is located (Matsumoto: see for example, Column 24 Line 25 – 28 and Column 24 Line 60 – 65).

45. As per claim 94, Matsumoto teaches the claimed invention as described above (see claim 87). Matsumoto further teaches the plurality of second-level system devices is arranged and constructed to encrypt at least a segment of the session authentication information using one of an intrakey and an interkey when the encrypted session authentication information is forwarded to a system device in a zone in which the forwarding device is located (Matsumoto: see for example, Column 12 Line 35 – 38, Column 12 Line 44 – 46; & Column 24 Line 25 – 28, Column 6 Line 9 – 13 and Column 5 Line 47 – 55 and Column 24 Line 56 – 65: Matsumoto first teaches the authentication information must be stored with encryption form. Matsumoto further teaches each zone uses different encryption / decryption keys).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

46. Claims 83 and 84 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan (Patent Number: 6128389), hereinafter referred to as Chan, in view of Jobst (Patent Number: US 6707915 B1), hereinafter referred to as Jobst.

47. As per claim 83, Chan teaches a system comprising:

a. a key management facility, arranged and constructed to store an authentication key for each mobile station residing in the system (Chan: see for example, Column 4 Line 17 – 35 & Figure 2 Element 204: SAMS is a Secured Authentication Management System);

b. a user configuration server, operably coupled to the key management facility, arranged and constructed to store and distribute session authentication information for each mobile station residing in the system (Chan: see for example, Column 11 Line 53 – 55 & Figure 2 Element 206: SAC stores the shared secret data signal per mobile station identification data unit);

c. a zone manager, operably coupled to the user configuration server, arranged and constructed to store relevant session authentication information for a zone managed by the zone manager and to distribute the relevant session authentication information to a home location register within a zone controller for the zone (Chan: see for example, Figure 2 Element 106C: MSC is another possible form of zone manager because a zone (location area or service area) is a pact of the MSC service area);

48. Chan does not teach the key management facility, user configuration server, and the zone manager are arranged and constructed to provide the session authentication information to each other or to a zone in the event of a fault in the system.

49. Jobst teaches:

d. wherein the key management facility, user configuration server, and the zone manager are arranged and constructed to provide the session authentication information to each other or to a zone in the event of a fault in the system (Jobst: see for example, Column 2 Line 28 – 33: Jobst teaches the cellular network would send MM IDENTITY REQUEST message to the mobile station in the case of system failures. This would evidently make key management facility, user configuration server, and the zone manager are arranged and constructed to provide the session authentication information to each other or to a zone as in the normal MM IDENTITY REQUEST upon mobile station location update);

50. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Jobst within the system of Chan because Jobst teaches how to handle the system fault in the cellular network in order to to effectively identify the failures in the cellular system (Jobst: see for example, Column 2 Line 28 – 33).

51. Chan as modified further teaches:

e. wherein the home location register is arranged and constructed to continue to provide authentication and support secure communications in the event of a fault at any of the key management facility, user configuration server, and the zone manager (Jobst: see for example, Figure 2 Element 110B and Column 2 Line 28 – 33: Jobst teaches, in cellular network, HLR is directly connected and operated with MSC/SAC/SAMA and thus should handle MM IDENTITY REQUEST message to the mobile station in the case of system failures assuming in the event of a fault at any of the key management facility, user configuration server, and the zone manager).

52. As per claim 84, Chan as modified teaches the claimed invention as described above (see claim 83). Chan as modified further teaches further teaches comprising a visited location register, arranged and constructed to continue to provide authentication and support secure communications in the event of a fault at any of the key management facility, user configuration server, and the zone manager, and wherein at least part of the relevant session authentication information is distributed to the visited location register (Jobst: see

for example, Figure 2 Element 110B and Column 2 Line 28 – 33: Jobst teaches, in cellular network, VLR/HLR is directly connected and operated with MSC/SAC/SAMA and thus should handle MM IDENTITY REQUEST message to the mobile station in the case of system failures assuming in the event of a fault at any of the key management facility, user configuration server, and the zone manager).

53. Claims 7, 9, 13, 20, 28, 30, 33 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Terrestrial Trunked Radio (TETRA) Voice Plus Data (V+D) Part 7: Security" (EN 300 392-7 V2.0.19, 2000-11), hereinafter referred to as TETRA-2000.

54. As per claims 7 and 28, TETRA-2000 teaches the claimed invention as described above (see claims 2 and 23 respectively). TETRA-2000 further teaches the derived cipher key (DCK) is stored at a visited location register (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 & Line 9 – 10 and Figure 1: TETRA-2000 teaches the protocol exchange and DCK is generated at the authentication center. TETRA-2000 discloses ensuring the A-key (authentication-key) of MS is never visible outside the authentication center. This implies the DCK can be distributed outside the authentication center including VLR, HLR and etc).

55. TETRA-2000 does not disclose expressly the derived cipher key (DCK) is encrypted by an intrakey.

56. However, TETRA-2000 teaches common ciphering key (CCK) can be encrypted (or sealed) by DCK (TETRA-2000: see for example, Section 6.5.1.3 and Section 4.2.3 Line 8 – 9).

57. Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify encrypting CCK with DCK to accommodate encrypting DCK with CCK because (a) Key encrypting key (KEK) can enhance the security on transferring the sensitive information, especially both of DCK and CCK are independently generated and (b) TETRA-2000 teaches CCK (common ciphering key) can be used as either an intrakey within the same zone or as interkey when moving to different zones depending on the CCK_id (CCK identification code for different location areas LA) (TETRA-2000: see for example, Section 6.5.1.3 and Section 4.2.3 Line 6).

58. As per claims 9 and 30, TETRA-2000 teaches the claimed invention as described above (see claims 2 and 23 respectively). TETRA-2000 further teaches the derived cipher key is stored at a home location register (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 & Line 9 – 10 and Figure 1: TETRA-2000 teaches the protocol exchange and DCK is generated at the authentication center. TETRA-2000 discloses ensuring the A-key (authentication-key) of MS is never visible outside the authentication center. This implies the DCK can be distributed outside the authentication center including HLR, VLR and etc).

59. TETRA-2000 does not disclose expressly the derived cipher key (DCK) is encrypted by an intrakey.

60. However, TETRA-2000 teaches common ciphering key (CCK) can be encrypted (or sealed) by DCK (TETRA-2000: see for example, Section 6.5.1.3 and Section 4.2.3 Line 8 – 9).

61. Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify encrypting CCK with DCK to accommodate encrypting DCK with CCK because (a) Key encrypting key (KEK) can enhance the security on transferring the sensitive information, especially both of DCK and CCK are independently generated and (b) TETRA-2000 teaches CCK (common ciphering key) can be used as either an intrakey within the same zone or as interkey when moving to different zones depending on the CCK_id (CCK identification code for different location areas LA) (TETRA-2000: see for example, Section 6.5.1.3 and Section 4.2.3 Line 6).

62. As per claim 13, 20, 33 and 40, TETRA-2000 teaches the claimed invention as described above (see claims 2, 16, 23 and 36 respectively). claim 13 does not further teach over claim 7 (or claim 9). Therefore, see rationale addressed above in rejecting claim 7 (or claim 9).

63. Claims 42 – 65 and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Terrestrial Trunked Radio (TETRA) Voice Plus Data (V+D) Part 7: Security" (EN 300 392-7 V2.0.19, 2000-11), hereinafter referred to as TETRA-2000, in view of Matsumoto (Patent Number: 6134431), hereinafter referred to as Matsumoto.

64. As per claim 42, TETRA-2000 teaches a system comprising: a first system device in a first zone of the system, the first system device comprised of memory for storing:

a. first zone session authentication information (TETRA-2000: see for example, Figure 1 & Figure 2, Section 4.1.2 and Section 4.1.3);

b. a first key for encrypting at least one of key material and a part of the first zone session authentication information for transport in real-time to another system device in the first zone (TETRA-2000: see for example, Section 4.2.6 Line 6 – 10).

c. a second key for encrypting at least a segment of the first zone session authentication information for transport to a system device in a zone other than the first zone (TETRA-2000: see for example, Section 6.5.1.3 and Section 4.2.3 Line 6: TETRA-2000 teaches CCK (common ciphering key) can be used as either an intrakey within the same zone or as interkey when moving to different zones depending on the CCK_id (CCK identification code for different location areas LA).

65. TETRA-2000 does not disclose expressly a second system device comprised of memory for storing the first zone session authentication information at least partially in an encrypted form.

66. Matsumoto teaches a second system device comprised of memory for storing the first zone session authentication information at least partially in an

encrypted form (Matsumoto: see for example, Column 12 Line 35 – 38, Column 12 Line 44 – 46, and Figure 1 Element 111 & Figure 9).

67. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Matsumoto within the system of TETRA-2000 because Matsumoto teaches a personal or mobile station authentication system and authentication method with enhanced security on sensitive data storages (Matsumoto: see for example, Column 12 Line 35 – 38, Column 1 Line 5 – 13).

68. As per claims 43 and 53, TETRA-2000 as modified teaches the claimed invention as described above (see claims 42 and 52 respectively). TETRA-2000 as modified further teaches the first system device is a zone controller (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 and Figure 1: TETRA-2000 teaches the protocol exchange is between the authentication center and mobile station. Therefore, it is evident that HLR/VLR (or zone controller) and base station should all be involved to carry out this authentication protocols).

69. As per claims 44 and 54, TETRA-2000 as modified teaches the claimed invention as described above (see claims 42 and 52 respectively). TETRA-2000 as modified further teaches the first system device is a visited location register (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 and Figure 1: TETRA-2000 teaches the protocol exchange is between the authentication center and mobile station. Therefore, it is evident that HLR/VLR (or zone controller) and base station should all be involved to carry out this authentication protocols).

70. As per claims 45 and 55, TETRA-2000 as modified teaches the claimed invention as described above (see claims 42 and 52 respectively). TETRA-2000 as modified further teaches the first system device is a home location register (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 and Figure 1: TETRA-2000 teaches the protocol exchange is between the authentication center and mobile station. Therefore, it is evident that HLR/VLR (or zone controller) and base station should all be involved to carry out this authentication protocols).

71. As per claims 46 and 60, TETRA-2000 as modified teaches the claimed invention as described above (see claims 42 and 59 respectively). TETRA-2000 as modified further teaches the second system device is a zone manager (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 and Figure 1: TETRA-2000 teaches the protocol exchange is between the authentication center and mobile station. Therefore, it is evident that MSC (as one type of zone manager) in its associated service area (or zone) should all be involved to carry out this authentication protocols).

72. As per claims 47 and 56, TETRA-2000 as modified teaches the claimed invention as described above (see claims 42 and 52 respectively). TETRA-2000 as modified further teaches another system device in the first zone is any of a base station, a base site, and a TETRA site controller (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 and Figure 1: TETRA-2000 teaches the protocol exchange is between the authentication center and mobile station. Therefore, it is evident that HLR/VLR (or zone controller) and base station should all be involved to carry out this authentication protocols).

73. As per claims 48 and 57, TETRA-2000 as modified teaches the claimed invention as described above (see claims 42 and 52 respectively). TETRA-2000 as modified further teaches the first zone session authentication information is stored at least partially encrypted in the first system device (Matsumoto: see for example, Column 12 Line 35 – 38, Column 12 Line 44 – 46, and Figure 1 Element 111 & Figure 9).

74. As per claims 49 and 58, TETRA-2000 as modified teaches the claimed invention as described above (see claims 42 and 52 respectively). TETRA-2000 as modified further teaches the first key is an intrakey associated with the first zone (Matsumoto: see for example, Column 24 Line 25 – 28, Column 6 Line 9 – 13 and Column 24 Line 56 – 65 & Figure 14 Elemnt 110-a/b: Matsumoto further teaches each zone uses different encryption / decryption keys and thereby the first key is an intrakey associated with the first zone).

75. As per claim 59, TETRA-2000 as modified teaches the claimed invention as described above (see claim 52). TETRA-2000 as modified further teaches a fourth system device comprised of memory for storing the second zone session authentication information at least partially in encrypted form (Matsumoto: see for example, Column 12 Line 35 – 53).

76. As per claim 50, TETRA-2000 as modified teaches the claimed invention as described above (see claim 42). TETRA-2000 as modified further teaches the first key is an interkey (TETRA-2000: see for example, Section 6.5.1.3 and Section 4.2.3 Line 6: TETRA-2000 teaches CCK (common ciphering key) can be used as either an intrakey within the same zone or as interkey when moving to

different zones depending on the CCK_id (CCK identification code for different location areas LA).

77. As per claim 51, TETRA-2000 as modified teaches the claimed invention as described above (see claim 42). TETRA-2000 as modified further teaches the second key is an interkey (TETRA-2000: see for example, Section 6.5.1.3 and Section 4.2.3 Line 6: TETRA-2000 teaches CCK (common ciphering key) can be used as either an intrakey within the same zone or as interkey when moving to different zones depending on the CCK_id (CCK identification code for different location areas LA).

78. As per claim 52, TETRA-2000 as modified teaches the claimed invention as described above (see claims 42). Claim 52 does not further teach over claim 42. Therefore, see rationale addressed above in rejecting claim 42.

79. As per claim 61, TETRA-2000 as modified teaches the claimed invention as described above (see claim 59). TETRA-2000 as modified further teaches comprising a fifth system device comprised of memory for storing system session authentication information comprising at least the first zone session authentication information and the second zone session authentication information at least partially in encrypted form (Matsumoto: see for example, Column 5 Line 49 – 51: The plurality of mobile stations are evidently covered by different zones).

80. As per claim 62, TETRA-2000 as modified teaches the claimed invention as described above (see claim 61). TETRA-2000 as modified further teaches the fifth system device is a user configuration server (Matsumoto: see for example,

Figure 14 Element 103-a / 103-b & Element 100 and Column 47 Line 47 – 55: The exchange operates as a configuration server to couple to the key management device to store and distribute session authentication information for each mobile station residing in the system).

81. As per claim 63, TETRA-2000 as modified teaches the claimed invention as described above (see claim 61). TETRA-2000 as modified further teaches a sixth system device comprised of: memory for storing authentication key information; a processor, operably coupled to the memory, the processor arranged and constructed to generate the system session authentication information from the authentication key information, and encrypt the system session authentication information for transport to at least the fifth system device in non-real-time (Matsumoto: see for example, Column 12 Line 44 – 46, and Figure 1 Element 111 & Figure 9: Key Database as a storage device for access in a non-real-time manner).

82. As per claim 64, TETRA-2000 as modified teaches the claimed invention as described above (see claim 63). TETRA-2000 as modified further teaches the sixth system device is an authentication center (Matsumoto: see for example, Figure 1 Element 104).

83. As per claim 65, TETRA-2000 as modified teaches the claimed invention as described above (see claim 63). TETRA-2000 as modified further teaches the sixth system device is a key management facility (Matsumoto: see for example, Figure 1 Element 104 and Element 111).

84. As per claim 67, TETRA-2000 as modified teaches the claimed invention as described above (see claim 63). TETRA-2000 as modified further teaches the session authentication information comprises at least two keys utilized in an encryption authentication process (See addressed claim 42 above).

85. Claim 70 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto (Patent Number: 6134431), hereinafter referred to as Matsumoto, and in view of Matyas (Patent Number: 5164988), hereinafter referred to as Matyas.

86. As per claim 70, Matsumoto teaches the claimed invention as described above (see claim 69). Matsumoto does not teach at least one of the plurality of keys is encrypted by a hardware-based encryption device.

87. Matyas teaches at least one of the plurality of keys is encrypted by a hardware-based encryption device (Matyas: see for example, Column 6 Line 23 – 25).

88. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Matyas within the system of Matsumoto because Matyas discloses a hardware encryption method that can improve the performance and enhance the security.

89. Claim 66 is rejected under 35 U.S.C. 103(a) as being unpatentable over "Terrestrial Trunked Radio (TETRA) Voice Plus Data (V+D) Part 7: Security" (EN

300 392-7 V2.0.19, 2000-11), hereinafter referred to as TETRA-2000, in view of Matsumoto (Patent Number: 6134431), hereinafter referred to as Matsumoto, and in view of Matyas (Patent Number: 5164988), hereinafter referred to as Matyas.

90. As per claim 66, TETRA-2000 as modified teaches the claimed invention as described above (see claim 63). TETRA-2000 as modified does not teach the authentication key information is hardware encrypted before storage in the sixth device.

91. Matyas teaches the authentication key information is hardware encrypted before storage in the sixth device (Matyas: see for example, Column 6 Line 23 – 25).

92. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Matyas within the system of TETRA-2000 as modified because Matyas discloses a hardware encryption method that can improve the performance and enhance the security.

93. Claims 85 and 86 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan (Patent Number: 6128389), hereinafter referred to as Chan, in view of Jobst (Patent Number: US 6707915 B1), hereinafter referred to as Jobst, and in view of "Terrestrial Trunked Radio (TETRA) Voice Plus Data (V+D) Part 7: Security" (EN 300 392-7 V2.0.19, 2000-11), hereinafter referred to as TETRA-2000.

94. As per claim 85, Chan as modified teaches the claimed invention as described above (see claim 83). Chan as modified further teaches the zone controller generates a derived cipher key from the session authentication information during an authentication process (TETRA-2000: see for example, Figure 1: TETRA-2000 teaches derived cipher key (DCK1) is generated at authentication centre. Zone controller can be part of the process of authentication centre to generate derived cipher key (DCK1)).

95. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of TETRA-2000 within the system of Chan as modified because TETRA-2000 Part 7 discloses the terrestrial trunked radio (i.e. cellular communications) on security aspect especially on authentication process).

96. As per claim 86, Chan as modified teaches the claimed invention as described above (see claim 83). Chan as modified further teaches the session authentication information comprises at least two keys utilized in an encryption authentication process (TETRA-2000: see for example, Section 4.2.3 Line 6 and Section 6.5.1.3 Line 2 – 5: TETRA-2000 discloses different location area (LA or Zone) can have distinct common ciphering keys).

97. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of TETRA-2000 within the system of Chan as modified because TETRA-2000 Part 7 discloses the terrestrial trunked radio (i.e. cellular communications) on security aspect especially on authentication process).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100